

Serverzertifikat beantragen

Erzeugen Sie eine Zertifikatanfrage (CSR) mit den unten genannten Daten (hier als Ausschnitt einer OpenSSL Config für einen CSR). Eine einfache und schnelle Möglichkeit hierzu bietet das [Certmake-Tool des ZIMK](#).

```
countryName           = DE
stateOrProvinceName  = Rheinland-Pfalz
localityName          = Trier
organizationName      = Universitaet Trier
```

Für die Beantragung eines Zertifikates benötigen Sie zwingend einen Account im HARICA Certificate Manager.

1. Gehen Sie auf <https://cm.harica.gr> und klicken Sie auf Academic Login.

Login

New to HARICA? [Sign Up](#)

Email address

Password

 
[Forgot password?](#)

Login

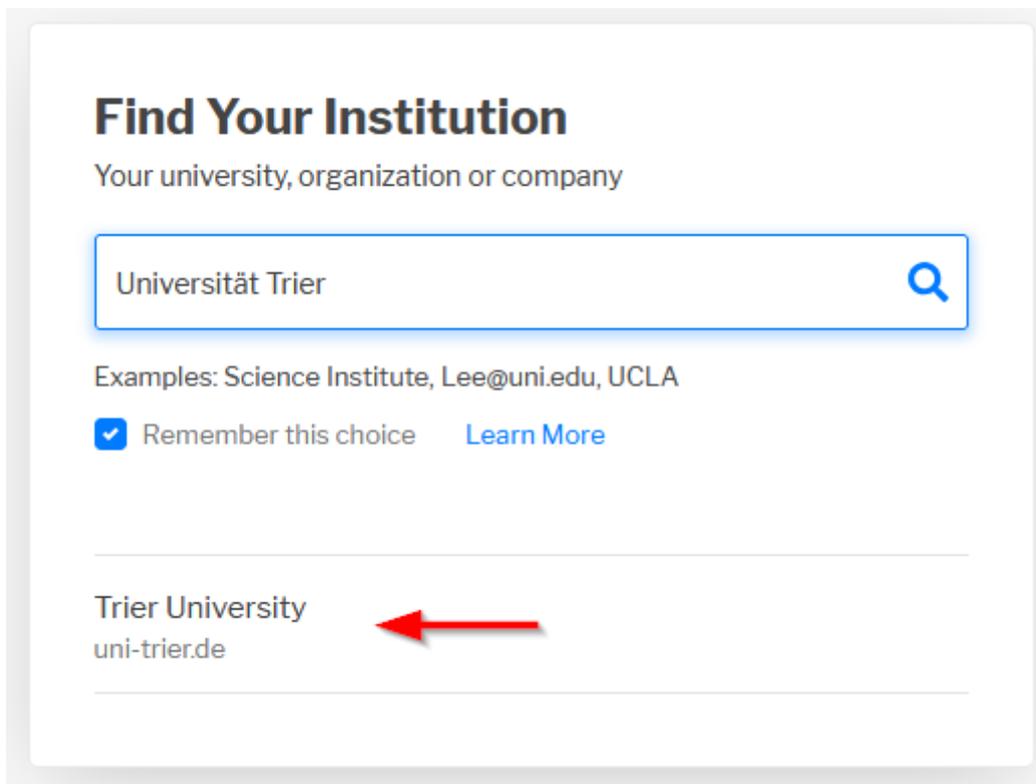
Or

 **Academic Login**

 **Sign in**

GREEK UNIVERSITIES NETWORK (GUnet)
General Commercial Registry Number: 160729401000

- Suchen Sie nach der Universität Trier, indem Sie im Suchfeld „Universität Trier“ eingeben und anschließend auf den Eintrag „Trier University – uni-trier.de“ klicken (s. Bild).



Find Your Institution
Your university, organization or company

Universität Trier

Examples: Science Institute, Lee@uni.edu, UCLA

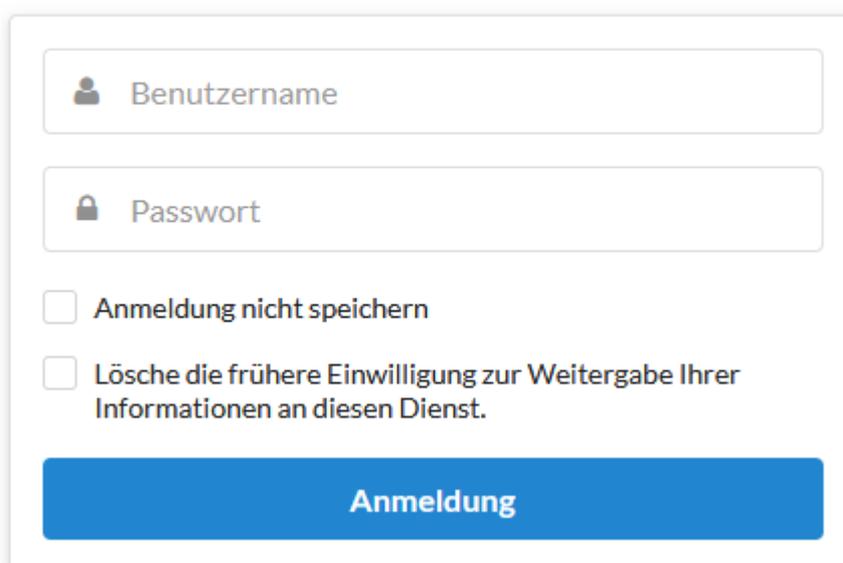
Remember this choice [Learn More](#)

Trier University
uni-trier.de

Sie werden zu der Shibboleth-Anmeldung des ZIMK weitergeleitet.

- Geben Sie nun bitte Ihre ZIMK-Anmeldeinformationen ein.

Anmelden bei HARICA



Benutzername

Passwort

Anmeldung nicht speichern

Lösche die frühere Einwilligung zur Weitergabe Ihrer Informationen an diesen Dienst.

Anmeldung

- Bitte akzeptieren Sie im nächsten Schritt die Weitergabe der benötigten Informationen an den Anbieter von GÉANT TCS, HARICA

Sie sind nun im HARICA Certificate Manager angemeldet und können nun ein Zertifikat beantragen, folgen Sie hierzu der entsprechenden Anleitung.

1. Wählen Sie links unter Certificate Requests "**Server**" durch Anklicken aus.

Vergeben Sie einen Anzeigenamen für Ihre Zertifikatsübersicht in HARICA (beispielsweise der CN, später änderbar). Hinweis: die Bezeichnung server im Bild ist nur ein Beispiel.

Tragen Sie unter Add Domains den Serverhostnamen (Common Name = CN) ein.

Der Haken vor Include server.uni-trier.de without additional cost sollte deaktiviert werden, wenn diese Domain nicht benötigt wird (Standardfall).

ACHTUNG: Alternative Namen (Subject Alternative Name = SAN) werden nicht aus dem CSR übernommen. Diese müssen unter + Add more domains angegeben werden.

Die Anzahl der SubjectAlternativeNames ist derzeit auf **20** begrenzt.

Klicken Sie auf Next.

My Dashboard

eSign Documents

Certificate Requests

eSignatures

eSeals

Server

Code Signing

Email

Client Authentication

More

Validated Information

Data privacy statement

Help / Guides

Server Certificates / Request new certificate

1. Request 2. Validate 3. Retrieve

Domains Product Details Authorization Summary Submit

Friendly name (optional)
A custom label to help you identify this certificate in your dashboard

server.uni-trier.de

Add Domains Manually or via Import 
supported: .onion v3, Wildcard, Internationalized Domain Name (IDN)

server.uni-trier.de ✓

Include **www.server.uni-trier.de** without additional cost.

+ Add more domains optional

The maximum number of domains allowed per request is 20.

Next

2. Wählen Sie bei Product die Option "For enterprises or organizations (OV)" durch Anklicken von Select aus.

For enterprises or organizations (OV)

SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:

- One or more domains
- Information of your organization that owns/controls the domains

Select

Free

3. Die ausgewählte Option "For enterprises or organizations (OV)" wird angezeigt, klicken Sie auf Next.

Select the type of your certificate Edit

For enterprises or organizations (OV)
SSL/TLS certificate that is used for secure communication between a web server and a client's browser. Includes:

- One or more domains
- Information of your organization that owns/controls the domains

Selected
Free

[← Back](#) **Next**

4. Die Angaben zu unserer Organisation, der Universität Trier, werden angezeigt, Klicken Sie auf Next.

Organization information

Legal name
Universitaet Trier

Country
DE

State or province
Rheinland-Pfalz

[← Back](#) **Next**

5. Die Angaben zum Zertifikat werden angezeigt, prüfen Sie diese und bestätigen Sie sie durch Setzen des Hakens und Klicken Sie dann auf Next.

Review the application before submitting

Certificate Type
SSL OV

Service Duration
1 year

Domains
server.uni-trier.de

Organization Details
Legal name: Universitaet Trier
State or province: Rheinland-Pfalz
Country: DE



I, *Vorname Name*, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

[← Back](#)

[Next](#)

6. Wählen Sie die Option "Submit CSR manually". Den notwendigen CSR (Certificate Signing Request) und einen Privaten Schlüssel müssen Sie selbst erstellt haben.

Die Verwendung der Option "Auto-generate CSR" bei dem die Erzeugung des Privaten Schlüssels im Browser erfolgt, wird nicht empfohlen.

Submit Request

? What is a CSR?

Auto-generate CSR

Create your Private Key directly in your browser, and your CSR will be auto-generated

OR

Submit CSR manually

Use your (already created) CSR and submit it here.

I, *Vorname Name*, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

[← Back](#) [Submit request](#)

7. Fügen Sie den durch Sie erzeugten CSR in das entsprechende Feld ein, setzen Sie den Haken bei der Zustimmung zu den Regularien und Klicken sie auf Submit Request.

Anschließend sehen Sie den Request im HARICA Dashboard. Dieser muss jetzt durch einen HARICA Approver des ZIMK bearbeitet und genehmigt werden.

Submit Request

? What is a CSR?

Auto-generate CSR

OR

Submit CSR manually

Use your (already created) CSR and submit it here.

```
-----BEGIN CERTIFICATE REQUEST-----
sadgsdhjdtjkdztzjkdtkztzk...

.....sdfasedgshgsdfhjsrfhsfgjfgjg
-----END CERTIFICATE REQUEST-----
```

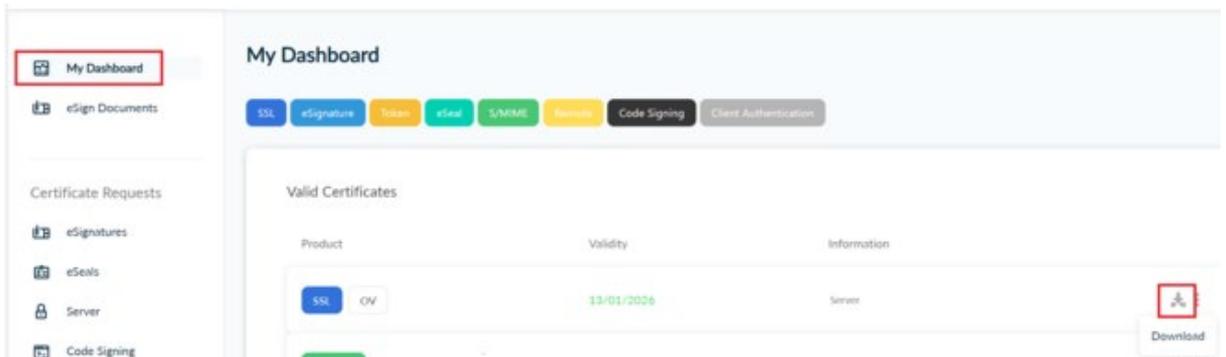


I, *Vorname Name*, declare that I read and agree with, by submitting this request, the [Terms of Use](#) and the [Certification Practices](#) of HARICA. I also agree that HARICA shall process, use and store the data from this request in accordance with the [Data Privacy Statement](#).

[← Back](#)

[Submit request](#)

8. Nach der Genehmigung des Zertifikatsantrages erhalten Sie vom HARICA Certificate Manager (CM) noreply@harica.gr
 - eine E-Mail (Betreff: E-Mail-Adresse des angemeldeten Accounts - SSL OV Certificate has been issued), die die Ausstellung des Zertifikates bestätigt.
 - eine E-Mail (Betreff: HARICA - Your certificate is ready), die aussagt, dass das Zertifikat bereit steht und über das Dashboard heruntergeladen werden kann.
9. Klicken Sie auf den in der Mail enthaltenen Link <https://cm.harica.gr/MyDashboard> und melden Sie sich am HARICA Certificate Manager an. Klicken Sie auf das Download-Symbol.



10. Wählen Sie das passende Format aus und laden Sie sich die entsprechende Datei herunter und installieren Sie das Zertifikat auf Ihrem Server. Über den Button "PEM bundle" erhält man eine Datei, die für Webserver wie Apache oder nginx direkt verwendbar ist.

Certificate



Details **Download** **Revocation** **Notifications** **Order**

You can download your Certificate in a variety of formats, depending on your needs.

Format	Description
PEM	Typical text format
DER	Typical binary format
DER CA	Typical binary format of the Issuing Authority Certificate
PKCS#7 (chain)	Typical text format including all certificate chain
PEM bundle	Typical text format including all certificate chain along with the cross certificate

If your Certificate's Private Key is installed in a cryptographic device (token), you can download the DER and DER (CA) files and import them to your device through the token's management software. Otherwise, you can download the PEM, PEM bundle files and along with the Private Key file that you created earlier during the request process (privateKey.pem), visit <https://www.harica.gr/en/Tools/PemToP12> and convert them into a single .p12 file which is used by various operating systems/applications.